

AFFIDAVIT OF NICOLE SORRELL

I, Nicole Sorrell, being duly sworn, hereby state the following:

1. I am a Special Agent with the Department of Homeland Security, United States Immigration and Customs Enforcement, Homeland Security Investigations (“HSI”), assigned to the Boston Field Office, and have been so employed since 2009. I am assigned to the Cyber and Child Exploitation Group. As part of my duties, I am authorized to investigate violations of the laws of the United States, including criminal violations relating to child exploitation, child pornography, coercion and enticement, and transportation of minors, including but not limited to violations of 18 U.S.C. §§ 2422, 2423, 2251, and 2252A. I have received training in the investigation of child exploitation offenses, including child pornography, and have had the opportunity to observe and review examples of child pornography (as defined in 18 U.S.C. § 2256).
2. I submit this affidavit in support of an application for a complaint charging Matthew STEFANELLI (born 1989) for the possession of child pornography, in violation of 18 U.S.C. § 2252A(a)(5)(B), hereinafter the “Subject Offense.”
3. The statements in this affidavit are based, in part, on information provided by other investigators, law enforcement reports by other investigators that I have reviewed, information obtained from the service of administrative subpoenas, physical and electronic surveillance conducted by law enforcement, investigation and analysis by analysts and computer forensic professionals; and my own experience and training. This affidavit is intended to establish the requisite probable cause for the issuance of a criminal complaint and does not set forth all of my knowledge about this matter.

BASIS FOR PROBABLE CAUSE

4. The National Center for Missing and Exploited Children (“NCMEC”) is a private, nonprofit organization that, among other things, tracks missing and exploited children, and serves as a repository for information about child pornography. Companies that suspect child pornography has been stored or transmitted on their systems can report that information to NCMEC in a CyberTip.

5. On or about October 15, 2020, Google submitted CyberTipline Report No. 81433190 (hereinafter the “CyberTip”) to NCMEC. The incident was listed as “Child Pornography (possession, manufacture, and distribution),” and the incident time and date were listed as October 14, 2020 at 11:27:16 UTC.¹
6. The CyberTip included one image file, named “Google-CT-RPT-[REDACTED],” with an original filename of “[REDACTED].jpg,” (hereinafter the “Subject File”).
7. On December 10, 2020, I conducted a search of the relevant NCMEC database for the hash value of the Subject File, which resulted in a confirmed match for an “identified child.” NCMEC defines the “identified child” as the exact hash value being associated with an image or video of child pornography which depicts at least one child under the age of 18 previously identified by law enforcement.
8. On or about December 21, 2020, I viewed the Subject File pursuant to a warrant issued by the Court. The file contains an image depicting a prepubescent female with blonde hair, approximately 6-7 years old, lying completely naked and prone on a blanket. The child is facing away from the camera, with her exposed buttocks and genital area as the focal point of the image. Although the child’s face is not visible, she does not appear to have any indicators of puberty, such as hip development or body hair.
9. The CyberTip Report included the following user information regarding the account used to upload the suspected child pornography:
 - Name: Matthew Stefanelli
 - Mobile Phone: (xxx) xxx-7755 (the “7755 Phone”)²
 - Email Address: matt7le@gmail.com (Verified)
 - Email Address: mat7le@yahoo.com
10. On or about January 2, 2020, Verizon provided records identifying STEFANELLI as

¹ The CyberTip indicated that the time and date refer to the approximate date and time that Google became aware of the material.

² According to Google records, the account was verified. To do so, a Google user must provide a phone number and choose to receive a text or voice message with a 6-digit code. The user must input the code to verify their account. Users can also update their contact email, which would prompt Google to send a verification message to the new email to confirm the address. The user would be prompted to click a verification link to verify the email address.

associated with the email account “matt7le@gmail.com” and the -7755 Phone.

11. Public records indicated that STEFANELLI resided at 13 Church Street, Unit 1, Upton, Massachusetts since December 2019. According to Massachusetts RMV records, STEFANELLI has an active Massachusetts driver’s license which lists 13 Church Street as both his mailing and residential address.
12. Checks of a public records database revealed that an adult female (“Female #1”) also resided at 13 Church Street, Upton, Massachusetts.
13. On or about September 21, 2020, United States Postal Inspection Services (“USPIS”) informed HSI that STEFANELLI and Female #1 received mail at 13 Church St. Additionally, USPIS informed HSI Boston that Female #1 changed her mailing address to 13 Church St. on or about December 12, 2019.
14. On January 6, 2021, at approximately 6:15 a.m., agents executed a federal search warrant at the first floor unit of 13 Church Street, Upton, Massachusetts. STEFANELLI, Female #1, and Female #1’s two minor children were present in the home.
15. STEFANELLI agreed to speak with agents after agents advised him of his *Miranda* rights. During that recorded interview:³
 - a. STEFANELLI stated that the email account “matt7le@gmail.com” belonged to him. He stated that he had been locked out of that account for several months. He denied using that account to view child pornography.
 - b. STEFANELLI stated that his primary phone number was (xxx) xxx-7755.
 - c. STEFANELLI identified a Samsung Galaxy A20 mobile phone as his primary phone (the “Galaxy Phone”). Agents located the Galaxy Phone attached to a charger in the bedroom that STEFANELLI indicated that he shared with Female #1. He provided a numeric passcode to agents that could be used to unlock the phone in combination with his fingerprint.

³ Unless otherwise indicated, all statements set forth within this affidavit are summary in nature

- d. STEFANELLI also identified other phones found in the home as “older” phones that were used primarily by the children, including a Motorola phone that was password protected with the same password as the Galaxy Phone.

FORENSIC EXAMINATION OF THE GALAXY PHONE

16. Attempts to conduct a forensic data extraction of the Galaxy Phone were initially unsuccessful due to the fact that the device was not supported by the forensic tools available at that time.⁴
17. On or about May 3, 2020, HSI Special Agent Andrew Kelleher obtained a full file system data extraction of the Galaxy Phone. According to the data extraction, the phone number associated with the device was the -7755 Phone with an activation date of April 14, 2020.
18. During the review of the data extracted from the Galaxy Phone, approximately 33 image files depicting apparent child pornography were discovered in a cache folder,⁵ including the Subject File identified in the Google CyberTip.
19. The relevant file path appears to contain the cache folder for the application “eztools.calculator.photo.vault.” Open source searches revealed that this application is the “Calculator + Vault” for Android devices, a third-party application that can be downloaded from the “Google Play” store. It presents - and functions - as a calculator, but also functions as a place to store encrypted files, images and videos. In my training and experience, I know that these types of application are typically used to conceal images, videos, or other files from anyone else using the device. In order to access the hidden storage function, the user sets a passcode to encrypt the files, and these files are subsequently accessed by entering the chosen passcode followed by the

⁴ During this process of attempting to extract data at the residence, agents accessed the Galaxy Phone using the passcode provided by STEFANELLI, and then removed the passcode from the device as part of the forensic process. Agents placed the Galaxy Phone into “airplane” mode and disabled the WiFi and Bluetooth connections in order to prevent any network connections or any changes to the data on the device.

⁵ These files were initially located in the file path: \data\data\eztools.calculator.photo.vault\cache\image_manager_disk_cache. A cache folder is typically a place where an application or program will store copies of files that are frequently accessed to allow those files to load faster when requested by the user. The presence of these files in the cache folder of an application indicate that the files are likely contained within the application or were there at one time.

% symbol. It appears the user can also create and name different folders within the hidden portion of the application

20. In an effort to validate that this application was installed on the device and determine whether image files depicting child pornography were contained inside the application, Agent Kelleher powered on the Galaxy Phone and accessed the applications present on the device. Agent Kelleher observed an application entitled "Calculator+". Agent Kelleher accessed the "Calculator+" application by entering the same passcode that STEFANELLI previously provided for the Galaxy Phone (and the older Motorola phone).

21. Approximately 117 images of an adult female who I recognize to be Female #1 were stored within the "Calculator + Vault" application. There was also an image that appears to depict Female #1's two minor children. Both minors are laying on a bed,

[REDACTED]

[REDACTED]

22. Agent Kelleher observed images of child pornography within the hidden photo albums that appear to be the same as those identified in the cache folder.

23. Further forensic analysis revealed that these image files depicting child pornography were contained within the filesystem data extraction in an encrypted state. Agents were able to export the encrypted image files and decrypt those files using a publicly available tool. Approximately 20 image files depicting child pornography were discovered within the "Calculator + Vault" application on the Galaxy Phone.

Specifically, those images included:

i. Encrypted file name: "dd2607f0-5c98-4059-a966-fab0751b08d9"

The image depicts a nude prepubescent female who appears to be approximately 4-6 years old. The child is seen laying on a purple blanket on her stomach. Her legs are slightly spread apart exposing her vulva to the camera. It appears to be a visual match for the Subject File that was the subject of the CyberTip.

ii. Encrypted File Name: [REDACTED]

This image depicts a prepubescent female who appears to be approximately 6 to 8 years old. The child is sitting back on what appears

to be a piece of furniture with a floral pattern, and her face is visible. She is wearing a pink, yellow, and orange sleeveless article of clothing, with orange and yellow shorts. The child has her legs spread apart and knees raised up. One of her hands is pulling her shorts to the side, exposing her vulva to the camera.

iii. Encrypted File Name: [REDACTED]

This image depicts a nude prepubescent female who appears to be approximately 8 to 10 years old. The child is completely nude, laying on her back on a white and red striped rug. The prepubescent female's legs are slightly apart, exposing her vulva to the camera.

iv. Encrypted File Name: [REDACTED]

This image depicts a nude prepubescent female who appears to be approximately 8 to 10 years old. The child is seen laying on her back with various blankets with a striped pillow behind her back and head. She is completely nude, laying with her hands raised up by her head, and her legs spread apart. Her knees are bent with one raised up, exposing her vulva to the camera.

24. According to the markings on the rear of the Samsung Galaxy, the device was manufactured in Vietnam.

CONCLUSION

25. Based on the foregoing information, there is probable cause to believe that, on or about January 6, 2021, STEFANELLI knowingly possessed material that contained one or more images of child pornography, as defined in Title 18, United States Code, Section 2256(8), that involved a prepubescent minor and a minor who had not attained 12 years of age, and that had been mailed, and shipped and transported using any means and facility of interstate and foreign commerce and in and affecting interstate and foreign commerce by any means, including by computer, and that was produced using materials that had been mailed, and shipped and transported in and affecting interstate and foreign commerce by any means, including by computer, in violation of 18 U.S.C. § 2252A(a)(5)(B).



Nicole Sorrell
Special Agent
Homeland Security Investigations

Sworn and subscribed before me telephonically pursuant to
Fed. R. Crim. P. 4.1 this 13th day of July, 2021. 12:49 p.m.



HONORABLE DAVID H. KENNEDY
UNITED STATES MAGISTRATE JUDGE

